

AUG 04 2006

Attorney Docket No. 030282

REMARKS

Claims 1-16, 18-29, 31, 32, and 34 remain pending in the application. Applicant, by this paper, amends claims 16, 23, 27, 29, 31, 32, and 34. Applicant respectfully requests reconsideration and allowance of all pending claims.

DISCUSSION OF REJECTIONS UNDER 35 U.S.C. §112

Claim 31 was rejected under 35 U.S.C. §112, second paragraph, as indefinite for being dependent upon a canceled claim. Applicant amends claim 31 to depend from claim 29 and respectfully requests withdrawal of the rejection in light of the claim amendment.

DISCUSSION OF REJECTIONS UNDER 35 U.S.C. §103

Claims 16, 18, 21-24, 26, and 27 were rejected under 35 U.S.C. §103(a) as allegedly unpatentable over U.S. Patent No. 6,243,468 to Pearce et al. (hereinafter Pearce) in view of U.S. Patent No. 6,931,545 to Ta et al. (hereinafter Ta). Claims 1-15, 19, 20, 25, 28, 29, 31, and 32 were rejected under 35 U.S.C. §103(a) as allegedly unpatentable over Pearce in view of Ta, in further view of pages 303-307 of "How The Internet Works" by Gralla (hereinafter Gralla).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be reasonable expectation of success. Finally, the prior art reference, or references when combined, must teach or suggest all of the claim limitations.

The Pearce and Ta references, whether alone or in combination, fail to teach or suggest all features of claims 16, 18, 21-24, 26, and 27.

Claim 16 includes "obtaining a second identifier for the hardware, the second identifier identifying a non-specific hardware platform." Support for this claimed feature is found in Applicant's Specification, at page 4, paragraph [1024] ("Each different hardware platform is assigned a different hardware ID, but all instances or units of the same hardware platform have the same hardware ID....The software ID and hardware ID thus identify the software release and hardware platform, respectively, and *not specific instances of the software and hardware.*") (*emphasis added*).

In direct contrast, Pearce is directed to associating software with a particular instance of hardware in which it is originally installed. *See, Pearce*, Abstract ("...requiring each software

Attorney Docker No. 030282

product to be registered for a single computer.”). The hardware ID described in Pearce refers to an identification of a *specific instance* of a computer on which software is installed. Pearce states: “The software product 100 generates a hardware ID (H/W ID) that identifies a set of hardware components that make up the customer’s computer 32.” *Pearce*, at Col. 5, ll. 57-59. “The anti-piracy system is effective at stopping repeated installation of the same software product on multiple different machines.” *Id.*, at Col. 7, ll. 14-16. Pearce goes on to state: “If an unscrupulous customer attempts to install the product on another computer, the software product will determine the test and registration IDs do not match and will self lock.” *Id.*, at ll. 31-34 (the test ID is generated using the computer specific hardware ID).

Therefore, in direct contrast to Applicant’s claimed second identifier identifying a non-specific hardware platform, Pearce describes a hardware identifier that is used to identify a *specific instance* of a computer on which software is installed. Further, Pearce cannot be modified to operate with a non-specific hardware ID, because modifying Pearce in such a manner would render Pearce’s system unsuitable for its intended purpose.

Applicant respectfully requests reconsideration and allowance of claim 16, because Pearce and Ta, alone or in combination, fail to teach every claimed feature. Furthermore, it is improper to modify the teachings of Pearce to provide the claimed features because to do so would render the system of Pearce unsuitable for its intended purpose.

Claim 23 recites an apparatus that includes “a controller operative to generate a signature for the software, the first identifier, and the second identifier using cryptography and a first secure cryptographic key, wherein the signature is used to validate an association of the software with the hardware, the controller further configured to generate a certificate using a second secure cryptographic key, the certificate used to authenticate a certificate authority.” This claimed feature is not taught nor suggested by Pearce or Ta, alone or in combination.

The Examiner concedes that Pearce fails to describe generating a signature using a first cryptographic key. The Examiner also concedes that Pearce and Ta, whether alone or in combination, fail to teach or suggest a certificate. *See, Office Action*, at page 3, ll. 15-18. Furthermore, none of the cited references teaches nor suggests generating a signature using a first cryptographic key and a certificate using a second cryptographic key. Thus, claim 23 is believed to be allowable because the cited references fail to teach or suggest all of the claimed features.

Attorney Docket No. 030282

Claim 27 includes a similar feature of “means for generating a certificate associated with the first signature using cryptography and a second secure cryptographic key, wherein the certificate is used to authenticate a certificate authority.” Thus, claim 27 is believed to be allowable at least for the reasons provided above in relation to claim 23.

Claim 1 includes “authenticating a certificate with a first public key” and “validating the signature with a second public key from the certificate, wherein the association of the software with the hardware is validated if the signature is validated.” This combination of features is not taught nor suggested by Pearce, Ta, or Gralla, whether alone or in combination.

The Examiner concedes that Pearce and Ta fail to teach or suggest communication using public keys and certificates. The Examiner contends that Gralla teaches public key cryptography and digital certificates used to secure network communications, and that this description in Gralla makes obvious the use of cryptography and digital certificates to secure network communications.

However, Applicant’s claim is not directed to secure network communications, but instead, is directed to “validating software for hardware.” Even if there is some motivation to use secure network communication in Pearce and Ta, such secure network communication has no bearing on Applicant’s claimed method. There is nothing in secure network communications to even suggest that public key cryptography could be used in validating software for hardware. Indeed, there is nothing about secure network communications that would suggest to one of ordinary skill in the art to relate in any way a certificate with the validity of software. Furthermore, there is nothing in a general description of the Internet to suggest that one should include a second public key in a certificate which is authenticated using a first key.

The combination of Pearce, Ta, and Gralla fail to teach or suggest all claimed features, because the references, whether alone or in combination, fail to teach validating a signature associating software with hardware using a public key that is included in a certificate that is itself authenticated with a public key.

Moreover, there is no motivation to combine the teachings of Gralla with Pearce and Ta. The Examiner contends that the combination is obvious because Gralla describes public key cryptography in the context of the Internet, and a heretofore uncited reference, Mia, describes authenticating a message using a hash. *Office Action*, at page 4.

Attorney Docket No. 030282

The Examiner ignores the case law that states that the mere fact that references *can* be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). It is error to reconstruct the claimed invention from the prior art by using the claim as a "blueprint." When prior art references require selective combination to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight obtained from the invention itself. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 227 USPQ 543 (Fed. Cir. 1985).

The Examiner is clearly requiring a selective combination of the references. The Examiner cites to four pages from the hundreds of pages from Gralla. Moreover, the Examiner contends that select portions of those four pages from Gralla can be used by one of ordinary skill in the art to modify particular features of the combination of Pearce with Ta. Moreover, the Examiner contends that it would be obvious to modify a particular portion of Pearce (network communications) that is unrelated to software anti-piracy, and that the modification to the network communication portion of Pearce and Ta somehow teaches all features of a claimed method for validating software with hardware.

The Examiner argues that combining well known authentication techniques is well known in the art. Applicant respectfully requests the Examiner provide a specific example of certificates and public key encryption in the context of validating software with hardware.

Clearly, the Examiner fails to provide any motivation that even suggests the selective combination argued by the Examiner. Moreover, the Examiner fails to describe how the purported combination teaches every claimed feature.

Therefore, Applicant requests reconsideration and allowance of claim 1.

Claims 9, 14, 29, 32, and 34 include similar features of a certificate and a signature used to validating software with hardware, where distinct cryptographic keys are used for the signature and the certificate. Thus, claims 9, 14, and 19 are believed to be allowable at least for the reasons presented above in relation to claim 1.

Claims 2-8, 10-13, 15, 18-22, 24-26, 28, and 31 depend from one of claims 1, 9, 14, 16, 23, 27, or 29 and are believed to be allowable at least for the reason that they depend from an allowable base claim. The Examiner fails to even provide any particular description as to how the combination of references purports to describe every feature of each of the dependent claims.

Attorney Docket No. 030282

Thus, the Examiner fails to establish a *prima facie* case of rejection for the majority of the dependent claims. Applicant requests reconsideration and allowance of claims 2-8, 10-13, 15, 18-22, 24-26, 28, and 31.

REQUEST FOR ALLOWANCE

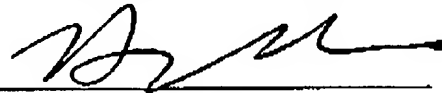
In view of the foregoing, Applicant submits that all pending claims in the Application are patentable. Accordingly, reconsideration and allowance of this Application is earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

If there are any fees due in connection with the filing of this response, please charge such fees to our Deposit Account No. 17-0026. If a fee is required for an extension of time under 37 C.F.R. 1.136 not accounted for, such an extension is requested and the fee should also be charged to our Deposit Account.

Respectfully submitted,

Dated: August 4, 2006
QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Facsimile: (858) 658-2502

By: _____


Howard H. Seo
Registration No. 43,106
(858) 845-5235